

Simon Bahne Paris, Esquire
Patrick Howard, Esquire (PA ID #88657)
Charles J. Kocher, Esquire (PA ID #93141)
SALTZ, MONGELUZZI, BARRETT
& BENDESKY, P.C.

One Liberty Place, 52nd Floor

1650 Market Place

Philadelphia, PA19103

Telephone: (215) 575-3986

Facsimile: (215) 496-0999

Email: sparis@smbb.com

phoward@smbb.com

ckocher@smbb.com

Attorneys for Plaintiff and the Proposed Class

PBT

18

2573

**UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF PENNSYLVANIA**

TRACEY KOPECKY, on behalf of herself and
all others similarly situated,

Plaintiff,

v.

FACEBOOK INC., a Delaware corporation;
CAMBRIDGE ANALYTICA LLC, a
Delaware limited liability company; and DOES
1-100,

Defendants.

Case No: _____

CLASS ACTION COMPLAINT

DEMAND FOR JURY TRIAL

Plaintiff, individually and as the representative of a class of similarly situated persons, by their undersigned counsel, alleges as follows:

NATURE OF THE CASE

1. This class action concerns a grievous and unprecedented breach of trust and invasion of privacy by which Facebook Inc. (“Facebook”) allowed Cambridge Analytica, LLC (“Cambridge Analytica”) and other unknown third party defendants access to, and the potential unlimited use of, vast amounts of sensitive personal information, including names, birthdates, locations, photos, videos, and likes (“Personal Information”)¹ from Facebook users without their consent.

2. Facebook operates a social networking platform where its users provide their Personal Information to Facebook under the belief and agreement that Facebook will safeguard that information, and that Facebook will share the information only with the persons, entities, and groups with whom the user consents. Instead of safeguarding this sensitive Personal Information, Facebook provided it to third party application (“app”) developers without user consent. Once the user data was in the possession of the third party app developers, Facebook exercised no control over how the app developer used the data.

3. Cambridge Analytica, through the use of one such third party app developer, obtained Personal Information from more than 87 million Facebook users which it thereafter used to create targeted political advertising and messaging in various United States elections. Moreover, this intentional massive data exfiltration is not an isolated incident but simply a high-profile exemplar.

¹ Facebook’s Personal Information list is included in full at ¶ 26, and includes: About me, Actions, Activities, Birthday, Check-ins, Education history, Events, Games activity, Groups, Hometown, Interests, Likes, Location, Notes, Online presence, Photo and video tags, Photos, Questions, Relationship details, Relationships, Religion, Politics, Status, Subscriptions, Website, and Work history. *See* <https://developers.facebook.com/docs/graph-api/changelog/archive>; *see also*, Iraklis Symeonidis, et al., “Collateral damage of Facebook Apps”, <https://eprint.iacr.org/2015/456.pdf>.

4. While the Cambridge Analytica incident has made the headlines only in recent months, Facebook has been aware of third party access, aggregation, distribution, and use of its users' sensitive Personal Information since at least 2010.

5. In 2011 the FTC finalized a formal complaint, alleging that Facebook's policies and practices threatened user privacy. Specifically, the complaint stated that Facebook's policies regarding third party developers were misleading and deceptive.² Facebook entered into a settlement with the FTC where Facebook is: 1) barred from making misrepresentations about the privacy or security of consumers' personal information; and 2) required to obtain consumers' affirmative express consent before enacting changes that override their privacy preferences.³ In response to this settlement, Mark Zuckerberg, founder and Chief Executive Officer of Facebook, made the following statement:

[T]his means we're making a clear and formal long-term commitment to do the things we've always tried to do and planned to keep doing -- giving you tools to control who can see your information and then making sure only those people you intend can see it.⁴

6. Facebook assures users that they own and control all the information they post on Facebook—a false and misleading statement. Facebook continues to induce its users into giving up information through its false promises of privacy while surreptitiously providing that information to third parties to generate revenue and while failing to take appropriate steps to safeguard Facebook users' Personal Information from unauthorized access, aggregation, distribution, and use.

²<https://www.ftc.gov/sites/default/files/documents/cases/2012/08/120810facebookcmpt.pdf>. The FTC complaint outlined the Commission's findings that Facebook made promises it did not keep when: 1) Facebook represented that third party apps its users installed would only have access to the user information needed to operate, when in fact, the apps could access nearly all of a user's personal data - data the apps didn't need; and 2) Facebook told users they could restrict sharing of data to limited audiences - for example with "Friends Only," when in fact, selecting "Friends Only" did not prevent their information from being shared with third party applications their friends used. *Id.*

³ <https://www.ftc.gov/news-events/press-releases/2011/11/facebook-settles-ftc-charges-it-deceived-consumers-failing-keep>.

⁴ <https://www.cnbc.com/2018/03/21/facebook-ceo-mark-zuckerbergs-statements-on-privacy-2003-2018.html>.

7. Only after public outcry has Facebook proposed remedial measures. Yet, these proposed measures remain feeble and hollow. None of these stopgap measures adequately remedy or prevent the improper and illegal conduct alleged. In fact, users' data remains dangerously unprotected and open to further abuse by third party app developers and anyone to whom these third party app developers distribute the users' data.

8. Defendants' disregard for the protection of Plaintiff's and class members' Personal Information has led Plaintiff to bring this suit to protect their privacy interests and those of the class.

JURISDICTION, VENUE, AND CHOICE OF LAW

9. Pursuant to 28 U.S.C. § 1331, this Court has original subject matter jurisdiction over the claims that arise under the Stored Communications Act, 18 U.S.C. §§ 2701, *et. seq.* This Court also has supplemental jurisdiction over the state law claims pursuant to 28 U.S.C. § 1367.

10. In addition to federal question jurisdiction, this Court also has diversity jurisdiction pursuant to 28 U.S.C. § 1332(d) under the Class Action Fairness Act ("CAFA"), because the amount in controversy exceeds \$5,000,000, exclusive of interest and costs, and at least one class member is a citizen of a state different from Defendants.

11. Venue is proper in this District pursuant to 28 U.S.C. § 1391 because Defendants do business in and are subject to personal jurisdiction in this District.

PARTIES

Plaintiff

12. Plaintiff Tracey Kopecky is a citizen of Wisconsin and currently resides in Holmen. Plaintiff has a Facebook account which she has maintained to the present day. Plaintiff's private information was exposed to Cambridge Analytica without her knowledge or consent.

Defendants

13. Defendant Facebook, Inc. ("Facebook"), a publicly traded company, is incorporated in the State of Delaware, with its principal executive offices located at 1601 Willow Road, Menlo Park, California 94025. Facebook is an online social media and social networking

service company founded in 2004. Facebook operates a social networking website that enables users to connect, share, and communicate with each other through text, photographs, and videos as well as to interact with third party apps such as games and quizzes on mobile devices and personal computers.

14. Defendant Cambridge Analytica LLC (“Cambridge Analytica”), a Delaware limited liability company, is a political consulting and “behavioral microtargeting” firm that combines data mining, data brokerage, and data analysis with strategic communication for the electoral process. It was founded in 2013 as a subsidiary of its parent company SCL Group, to participate in American politics. In 2014, Cambridge Analytica was involved in 44 U.S. political races. Cambridge Analytica does business throughout the United States, including in this District. Cambridge Analytica maintains offices in London, New York, and Washington, D.C.

15. Plaintiff does not know the true names of Defendants Does 1-100, inclusive, and therefore sues them by those fictitious names. Plaintiff is informed and believes, and on the basis of that information and belief alleges, that each of those defendants were proximately responsible for the events and happenings alleged in this Complaint and for Plaintiff’s injuries and damages.

FACTUAL BACKGROUND

A. Facebook’s Collection of Users’ Personal Information and Third Party Access

16. Since its inception in 2004, Facebook has grown to become synonymous with interconnectedness in the age of social media. Facebook now has over two billion monthly active users, with over 200 million in the United States alone.⁵ With each user sharing Personal Information in order to access the website, Facebook has become one of the world’s largest repositories of personal data.⁶

⁵ <https://www.statista.com/statistics/398136/us-facebook-user-age-groups/>;
<https://newsroom.fb.com/company-info/>.

⁶ <https://www.statista.com/statistics/398136/us-facebook-user-age-groups/>;
<https://newsroom.fb.com/company-info/>.

17. While Facebook may have started as a platform designed to service social connections, Facebook's focus has steadily shifted to data mining. Facebook's business model is now centered around finding ways to harness and sell the ability to influence its users' behavior.

18. In May 2007, Facebook unveiled Facebook Platform, calling on all developers to build the next-generation of applications with deep integration into Facebook, distribution across its "social graph," and an opportunity to build new business.⁷ Facebook CEO Mark Zuckerberg told the audience of 750 developers and partners: "Until now, social networks have been closed platforms. Today, we're going to end that. With this evolution of Facebook Platform, any developer worldwide can build full social applications on top of the social graph, inside of Facebook." Zuckerberg continued, "This is good for us because if developers build great applications then they're providing a service to our users and strengthening the social graph, [...]. This is a big opportunity. We provide the integration and distribution and developers provide the applications. We help users share more information and together we benefit."⁸

19. As a purported social media leader, Facebook knows the critical importance of protecting users' Personal Information from unauthorized access. Facebook also knows the multitude of harms that foreseeably flow to individual users when information is stolen or misused by criminals.

20. To its users, Facebook promotes and provides assurances of privacy and the ability for users to control what information is transmitted to third parties. Facebook has explicitly told its users that their Personal Information would not be sold, transferred, or otherwise shared to any advertisement network, data broker, or other advertising or monetization-related third party without their expressed consent.

⁷ <https://newsroom.fb.com/news/2007/05/facebook-unveils-platform-for-developers-of-social-applications/>. This unveiling took place at Facebook's first almost annual F8 conference, intended for developers and entrepreneurs who build products and services around the Facebook website.

⁸ *Id.*

21. Indeed, Facebook’s “Data Use Policy” emphasizes “trust” and states that “we don’t share information we receive about you with others unless we have ... received your permission [and] given you notice.”

22. The opening line of Facebook’s Statement of Rights and Responsibility is unambiguous in its recognition that Facebook users “own” their Personal Information and that users may rely on Facebook to protect that information from unwarranted disclosure:

1. Privacy

Your privacy is very important to us. We designed our Data Policy to make important disclosures about how you can use Facebook to share with others and how we collect and can use your content and information. We encourage you to read the Data Policy, and to use it to help you make informed decisions.

2. Sharing Your Content and Information

You own all of the content and information you post on Facebook, and you can control how it is shared through your privacy and application settings.⁹

23. Facebook’s CEO Mark Zuckerberg has also publicly acknowledged the importance of privacy on its platform—stating that people engage and share on Facebook because “they know their privacy is going to be protected.”¹⁰

24. A vital feature of Facebook is the appearance of control users have over their sensitive Personal Information. Facebook’s privacy settings purport to offer users degrees of control over the dissemination of their Personal Information. Specifically, Facebook gives users the option to share, privately with only certain individuals, with all of their Facebook friends, with friends of friends, or with all Facebook users.¹¹ Users reasonably expect their Personal Information will be accessible only to the extent they authorize such access.

⁹ Terms of Service, Statement of Rights and Responsibilities, FACEBOOK, <https://www.facebook.com/terms.php>.

¹⁰ Catherine Clifford, *Mark Zuckerberg 9 months ago: People share on Facebook because ‘they know their privacy is going to be protected’*, CNBC (April 3, 2018), <https://www.cnbc.com/2018/04/03/zuckerberg-on-facebook-and-privacy-before-cambridge-analytica-scandal.html>.

¹¹ Basic Privacy Settings & Tools: Selecting an Audience for Stuff You Share, Facebook, <https://www.facebook.com/help/325807937506242/> (last visited Apr. 30, 2018).

25. In 2010, Facebook released its Graph API (application programming interface), which is a developer, or app-level, interface touted as a revolution in large-scale data provision. The Graph API is the primary way to get data into and out of the Facebook platform. Graph API v.1.0, in effect from April 2010 to April 2015, converted Facebook users' Personal Information into quite literally "objects."¹²

26. Facebook's Graph API v.1.0 allowed third party app developers to access and store on third party servers, the following user data ("Personal Information"):¹³

¹² <https://medium.com/tow-center/the-graph-api-key-points-in-the-facebook-and-cambridge-analytica-debacle-b69fe692d747>.

¹³ *Supra*, fn. 1.

Basic Info (default)	Extended Profile Properties (xpP)		Extended Permissions (xP)
	User Data	Friends Data	
uid	user_about_me	friends_about_me	ads_management
name	user_actions.books	friends_actions.books	ads_read
first_name	user_actions.music	friends_actions.music	create_event
last_name	user_actions.news	friends_actions.news	create_note
link	user_actions.video	friends_actions.video	email
username	user_activities	friends_activities	export_stream
gender	user_birthday	friends_birthday	manage_friendlists
locale	user_checkins	friends_checkins	manage_notifications
age_range	user_education_history	friends_education_history	manage_pages
	user_events	friends_events	photo_upload
	user_friends	friends_games_activity	publish_actions
	user_games_activity	friends_groups	publish_checkins
	user_groups	friends_hometown	publish_stream
	user_hometown	friends_interests	read_friendlists
	user_interests	friends_likes	read_insights
	user_likes	friends_location	read_mailbox
	user_location	friends_notes	read_page_mailboxes
	user_notes	friends_online_presence	read_requests
	user_online_presence	friends_photo_video_tags	read_stream
	user_photo_video_tags	friends_photos	rsvp_event
	user_photos	friends_questions	share_item
	user_questions	friends_relationship_details	sis
	user_relationship_details	friends_relationships	status_update
	user_relationships	friends_religion_politics	video_upload
	user_religion_politics	friends_status	xmpp_login
	user_status	friends_subscriptions	
	user_videos	friends_website	
	user_website	friends_work_history	
	user_work_history		

27. Facebook's Graph API v.1.0 allowed third party app developers to access and collect Personal Information from users through the friends data scrape feature, including photos and videos, without users' consent, and even where a user's profile was set to private.

28. According to former Facebook platform operations manager, Sandy Parakilas, "tens or maybe even hundreds of thousands of developers" may have sought friends' permission data before such access was terminated in 2015.¹⁴ Parakilas explained how outside app developers have been able to access Facebook users' private information:

It's important to remember that apps on Facebook, when you use them, they ask you for permission to access specific kinds of data, whether it's your name or your e-mail address

¹⁴ <https://www.theguardian.com/news/2018/mar/20/facebook-data-cambridge-analytica-sandy-parakilas>.

or your friends list or photos or other information. And once you click “Allow” or tap “Allow,” all that information passes from Facebook to the application developer. And the problem is that, once the data goes to the developer, there is no insight into what the developer is doing with the data, and there is no control by Facebook as to what they do. This has been a known problem since 2010.¹⁵

29. As information is shared by these billions of unique users, Facebook is provided with sophisticated, exceedingly detailed data profiles. Facebook, through Graph API, permitted developers to tap into this abundance of Personal Information without any meaningful oversight and without Facebook users’ consent.

30. Facebook was aware of its lax approach to data protection because the majority of problems that have now come to the surface were meant to be features, not bugs. Facebook’s business model rests on collecting these highly personal and highly revealing data points and selling to third party app developers, without vetting or following up, the ability to use this data about individuals to target ads to them.

31. Facebook permitted third party app developers to improperly and illicitly harvest user data, purposely turning a blind eye while it continued to tout “trust,” “privacy,” and other pseudo-uplifting marketing speak to its Facebook users.¹⁶

32. A former Facebook platform operations manager had warned Facebook executives of this major risk of misuse of user data as early as 2011 but was discouraged from auditing third party developers’ use of Facebook users’ data. Regarding the recent headlines that Cambridge Analytica had illegally scraped Plaintiff’s and class members’ data to improperly influence and otherwise disrupt the outcome of the 2016 Presidential election that former manager stated: “It’s been painful watching . . . because I know they could have prevented it.”¹⁷

¹⁵ <https://www.cbsnews.com/news/sandy-parakilas-former-facebook-manager-warned-company-privacy-risks-in-2012/>.

¹⁶ Oliva Solon, *‘A grand illusion’: seven days that shattered Facebook’s facade*, THE GUARDIAN (March 24, 2018), <https://www.theguardian.com/technology/2018/mar/24/cambridge-analytica-week-that-shattered-facebook-privacy>.

¹⁷ Paul Lewis, *‘Utterly horrifying’: ex-Facebook insider says covert data harvesting was routine*, THE GUARDIAN (March 20, 2018), <https://www.theguardian.com/news/2018/mar/20/facebook-data-cambridge-analytica-sandy-parakilas>.

B. Cambridge Analytica's Harvesting of Facebook Users' Personal Information

33. In 2013, Alexander Nix was the leader of the special elections division of the Strategic Communication Laboratories Group ("SCL Group"), a London-based public relations firm that describes its expertise as "psychological warfare" and "influence operations."¹⁸ The same year, Mr. Nix met with Steven Bannon (former executive chairman of the "alt-right" news network Breitbart and former Trump advisor). They joined forces with Robert Mercer (U.S. hedge fund billionaire and Republican donor) in a scheme to use personality profiling to influence voting behavior.

34. With Mr. Mercer's \$15 million investment, Cambridge Analytica was born and their efforts to "bring big data and social media to an established military methodology— 'information operations'— then turn it on the U.S. electorate" soon began.¹⁹

35. Christopher Wylie, former employee of Cambridge Analytica, was a data expert who oversaw the misconduct complained of herein.

36. In 2014, Cambridge Analytica set out to acquire the behavioral data of American citizens. Mr. Wylie found that Cambridge University Psychometrics Center researchers had developed a technique to map personality traits based on Facebook users' profiles. The approach, the Psychometrics Center researchers said, could reveal more about a person than their parents or romantic partners knew.

37. To its credit, Cambridge University Psychometrics Center declined to work with Cambridge Analytica.

38. Mr. Wylie then solicited Dr. Aleksandr Kogan, then a psychology professor at Cambridge University. Kogan agreed to work with Cambridge Analytica; to harvest Facebook data "so that it could be matched to personality traits and voter rolls."²⁰

¹⁸ See, e.g., Sharon Weinberger, *You Can't Handle the Truth*, SLATE (Sept. 19, 2005), http://www.slate.com/articles/news_and_politics/dispatches/2005/09/you_cant_handle_the_truth.html.

¹⁹ Carole Cadwalladr, *The Cambridge Analytica Files 'I made Steve Bannon's psychological warfare tool': meet the data war whistleblower*, THE GUARDIAN (March 18, 2018), <https://www.theguardian.com/news/2018/mar/17/data-war-whistleblower-christopher-wylie-facebook-nix-bannon-trump> (last visited June 14, 2018).

²⁰ *Id.*

39. By June 2014, Cambridge Analytica had paid over \$800,000 for Dr. Kogan to begin surreptitiously harvesting Facebook user's Personal Information and transmit it to them.

40. Dr. Kogan created a U.K. company called Global Science Research, Ltd. ("GSR") and through GSR, created a Facebook app called "ThisIsYourDigitalLife"²¹ ("YDL app"). The YDL app consisted of a personality quiz hosted on Qualtric (an online survey platform) that required Facebook login credentials to complete.

41. Posing as an academic researcher, Cambridge Analytica and Dr. Kogan utilized Amazon's Mechanical Turk ("MTurk") program to recruit participants to complete the personality quiz. Participants were offered \$0.50-\$2.00 to complete the quiz.

42. When participants responded to Kogan's request and expressed interest in completing the personality quiz, Kogan sent them a link to his Facebook application. Participants then completed the personality quiz, but to receive payment they were told that they needed to allow the quiz app access to their Facebook data for academic purposes. "And not just theirs, but their friends' too. On average, each 'seeder'—the people who had taken the personality test, around 320,000 in total—unwittingly gave access to at least 160 other people's profiles, none of whom would have known or had reason to suspect. What the email correspondence between Cambridge Analytica employees and Kogan shows is that Kogan had collected millions of profiles in a matter of weeks."²² But no one "at Cambridge Analytica had checked that it was legal."²³

43. At no time did Cambridge Analytica, Dr. Kogan, or GSR inform participants that their Personal Information was going to be used for non-academic purposes, including the intended improper use for electoral targeting.

²¹ Different sources have called the app "thisismydigitallife" or have spelled the YDL app with different spacing variations but for all intents and purposes, Plaintiff is referring to the same app.

²² Carole Cadwalladr, *The Cambridge Analytica Files 'I made Steve Bannon's psychological warfare tool': meet the data war whistleblower*, THE GUARDIAN (March 18, 2018), <https://www.theguardian.com/news/2018/mar/17/data-war-whistleblower-christopher-wylie-facebook-nix-bannon-trump> (last visited June 14, 2018).

²³ Carole Cadwalladr, *The Cambridge Analytica Files 'I made Steve Bannon's psychological warfare tool': meet the data war whistleblower*, THE GUARDIAN (March 18, 2018), <https://www.theguardian.com/news/2018/mar/17/data-war-whistleblower-christopher-wylie-facebook-nix-bannon-trump> (last visited June 14, 2018).

44. At no time did Cambridge Analytica, Dr. Kogan, or GSR obtain permission from its YDL app users' Facebook friends to harvest their personal data.

45. Cambridge Analytica failed to inform or obtain permission because it knew it was not performing academic research; answers to the YDL app's personality quiz were not important. Instead, what it wanted and what it ultimately received, was access to the Personal Information of each YDL app user and *all* of that user's Facebook friends' Personal Information. While the exact information that GSR provided to Cambridge Analytica is unknown, GSR had access to all Personal Information available through Graph API v.1.0 including the names, video, images, and photos of millions of Facebook users.²⁴

46. The YDL app was so successful that from approximately 320,000 "seeders" who unwittingly completed the quiz, Defendant gained access to not only their Personal Information but also to over 87 million Facebook users' Personal Information.

47. The whistleblower, Mr. Wylie, confirms that there are receipts, invoices, emails, legal letters—records that showed how, between June and August 2014, Cambridge Analytica harvested the profiles of tens of millions of Facebook users.

48. The YDL app was used by Cambridge Analytica to create "psychographic" profiles which were then used to make predictions about people's behaviors and to create predictions about what people will do and what motivates them. This allowed Cambridge Analytica to design targeted political ads—using stolen Personal Information to play to unsuspecting users' preferences in efforts to influence their political views and choices.

²⁴ <https://medium.com/tow-center/the-graph-api-key-points-in-the-facebook-and-cambridge-analytica-debacle-b69fe692d747>.

C. Facebook Learns of YDL App's Data Collection and Fails to Act

49. Mr. Wylie confirms that Facebook should have known that the YDL app was collecting users' information at the time as its security protocols would have been triggered due to the enormous amount of data that the YDL app was pulling from Facebook's Graph API.

50. By the end of 2015, Facebook was notified that the data extracted by the YDL app had been transmitted to Cambridge Analytica. Instead of notifying its users, Facebook sat on this information for months taking no action. When Facebook finally took steps in mid-2016, Facebook's remedial action was limited.

51. Mr. Wylie, who responded to Facebook's request to delete the illicitly obtained data, was astonished by Facebook's lackluster response. Facebook made zero effort to get the data back and did nothing to confirm that the data was even deleted.

52. In the weeks leading up the 2016 presidential election, Mark Zuckerberg's trusted mentor and longtime investor, Roger McNamee, sounded the alarm about platform manipulation. Facebook executives brushed his concerns aside.²⁵

53. To date, all data improperly obtained by Cambridge Analytica still has not been deleted.

54. This mass data collection was not only permitted, but also incentivized by Facebook, which sought to encourage developers to build on its platform, which upon information and belief, financially benefitted Facebook.

D. Defendants' Wrongdoing Finally Exposed

55. Facebook's inadequate data security practices and systematic failure to enforce its own ineffective data security policies were exploited for financial and political gain by Cambridge Analytica and Doe Defendants.

56. On March 17, 2018, Defendants' actions were finally made public.

57. The Guardian published an article, based on information obtained from Mr. Wylie, which detailed Cambridge's mining of over 87,000,000 Facebook users' Personal

²⁵ Lila MacLellan, *Maybe Mark Zuckerberg shouldn't have blown off his mentor*, QUARTZ AT WORK (March 20, 2018), <https://work.qz.com/1233606/maybe-facebook-ceo-mark-zuckerberg-shouldnt-have-blown-off-his-mentor-roger-mcnamee/>.

Information and its employment of that data to target individuals with its psychological operations to influence their views during the 2016 presidential election.²⁶

58. After Defendants' wrongdoing was exposed, Facebook finally suspended Cambridge Analytica's and its affiliates' access to Facebook's platform.

59. Only in the aftermath of this news, Facebook has been attempting to salvage its brand and rebuild consumer trust by revamping its privacy policies.

60. Facebook's CEO Mark Zuckerberg publicly refused to appear before Parliament to answer questions regarding YDL. On the afternoon of April 4, 2018, after rebuffing Parliament, Facebook published a new data policy on its website. The new data policy is inadequate and so vague as that it continues to allow improper access to user data.

61. Facebook's stopgap measures fail to provide an adequate remedy or prevent further improper and illegal conduct. Personal Information already compromised remains dangerously vulnerable and open to further abuse. None of Facebook's measures constitute adequate notice to affected consumers. Further, Facebook has a history of failing to enforce its own data security policies.

E. Plaintiff's Experience

62. Plaintiff Tracey Kopecky was notified on April 10, 2018 through Facebook's Help Center that one of her friends had logged into the YDL app. Facebook's website informed Ms. Kopecky that information such as her public profile, Page likes, birthday, and current city was also likely shared with the YDL app and thus Cambridge Analytica. Facebook also informed Ms. Kopecky that a small number of people who logged into the YDL app also shared their own News Feed, timeline, posts, and messages which may have included posts and messages from Ms. Kopecky. Further, Mr. Ms. Kopecky's hometown may have been shared with Cambridge Analytica.

63. Plaintiff and class members had their Personal Information harvested from their Facebook profiles by Cambridge Analytica through use of the YDL app, either directly as a user of the app, or indirectly as a Facebook friend of a user of the app.

²⁶ *Id.*

64. Plaintiff and class members did not consent for the YDL app to have access to their Personal Information or else only consented for their information to be accessed for academic purposes.

65. Plaintiff and class members were harmed by Cambridge Analytica unlawfully obtaining their Personal Information, using such to psychologically profile them, and Cambridge Analytica directing its psychological operations at them in an effort to influence their views about, among other things, the 2016 Presidential Election.

66. Plaintiff and class members have been injured in a number of ways, including: (i) they have lost control over their Personal Information and how it is used, as promised by Facebook; (ii) the value of their Personal Information, for which there is a well-established market, has diminished because it is no longer private; (iii) their Personal Information has been misused and is vulnerable to continued misuse; and (iv) they will have to spend time and money securing their Personal Information, protecting their identities, monitoring their accounts and credit and/or paying for further identity theft protection services in the wake of Cambridge Analytica's harvesting of Personal Information, to make sure their identities were not stolen and mitigating misuse of their Personal Information.

CLASS ACTION ALLEGATIONS

67. Plaintiff incorporates by reference all allegations of the preceding paragraphs as though fully set forth herein.

68. Plaintiff brings this action on behalf of herself and all others similarly situated pursuant to Rule 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure.

69. Plaintiff seeks to represent the following Classes:

Nationwide Class

All persons who registered for Facebook in the United States and whose Personal Information was obtained by third parties through Facebook's Graph API's "extended permissions" functionality.

Wisconsin Sub-Class

All persons who registered for Facebook in Wisconsin and whose Personal Information was obtained by third parties through Facebook's Graph API's "extended permissions" functionality.

70. Excluded from the Class are Defendants, their current employees, coconspirators, officers, directors, legal representatives, heirs, successors and wholly or partly owned subsidiaries or affiliated companies; the undersigned counsel for Plaintiff and their employees; and the judge and court staff to whom this case is assigned. Plaintiff reserves the right to amend the definition of the Class if discovery or further investigation reveals that the Class should be expanded or otherwise modified.

71. **Numerosity and Ascertainability:** Plaintiff does not know the exact size of the Class or the identities of the Class Members since such information is the exclusive control of Defendants. Plaintiff believes that the Class encompasses approximately over 87,000,000 individuals who are geographically dispersed throughout the United States. The number of members in the Class are so numerous that joinder of all Class Members is impracticable. The names, addresses, and phone numbers of class members are identifiable through documents maintained by Defendants.

72. **Commonality and Predominance:** The action involves common questions of law and fact, which predominate over any question solely affecting individual Class Members, including:

- a. Whether Facebook gave Plaintiff and class members effective notice of its program to collect their Personal Information;
- b. Whether Defendants obtained consent from Plaintiff and class members to collect their Personal Information;
- c. Whether Defendants improperly collected Plaintiff's and class members' Personal Information;
- d. Whether Facebook represented that Plaintiff's and class members' Personal Information would be protected from disclosure absent their consent;
- e. Whether Facebook owes any duty to Plaintiff and class members with respect to maintaining, securing, or deleting their Personal Information;
- f. To what degree Facebook has the right to use Personal Information pertaining to Plaintiff and class members;

- g. Whether Facebook owed a legal duty to Plaintiff and the Class to exercise due care in collecting, storing, safeguarding, and/or obtaining their Personal Information;
- h. Whether Facebook breached a legal duty to Plaintiff and the Class to exercise due care in collecting, storing, safeguarding, and/or obtaining their Personal Information;
- i. Whether the egregious breach of privacy and trust alleged in the Complaint was foreseeable by Facebook;
- j. Whether Facebook intentionally exposed Plaintiff's and class members' Personal Information to Cambridge Analytica;
- k. Whether Defendants violated the Stored Communications Act;
- l. Whether Defendants violated Plaintiff's and class members' privacy rights;
- m. Whether Plaintiff and the Class are entitled to equitable relief, including, but not limited to, injunctive relief and restitution/disgorgement; and
- n. Whether Plaintiff and the Class are entitled to actual, statutory, or other forms of damages, and other monetary relief.

73. Defendants engaged in a common course of conduct giving rise to the legal rights sought to be enforced by this action and similar or identical questions of statutory and common law, as well as similar or identical injuries, are involved. Individual questions, if any, pale in comparison to the numerous common questions that predominate this action.

74. **Typicality:** Plaintiff's claims are typical of the other class members' claims because all class members were comparably injured through Defendants' substantially uniform misconduct as described above. Plaintiff is advancing the same claims and legal theories on behalf of herself and all other class members, and there are no defenses that are unique to Plaintiff. The claims of Plaintiff and class members arise from the same operative facts and are based on the same legal theories.

75. **Adequacy:** Plaintiff is an adequate Class representative because her interests do not conflict with the interests of the other members of the Classes she seeks to represent; Plaintiff

has retained counsel competent and experienced in complex class action litigation, and Plaintiff intends to prosecute this action vigorously. The Classes' interest will be fairly and adequately protected by Plaintiff and her counsel.

76. **Superiority:** A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. The damages or other financial detriment suffered by Plaintiff and the other class members are relatively small compared to the burden and expense that would be required to individually litigate their claims against Defendants, so it would be virtually impossible for the members of the Classes to individually seek redress for Defendants' wrongful conduct. Even if class members could afford individual litigation, the court system could not. Individualized litigation creates a potential for inconsistent or contradictory judgments, and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties, and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court.

CLAIMS FOR RELIEF

COUNT ONE

Violations of the Stored Communications Act 18 U.S.C. § 2701, *et. seq.*

77. Plaintiff incorporates by reference all allegations of the preceding paragraphs as though fully set forth herein.

78. Plaintiff, individually and on behalf of class members, asserts violations of 18 U.S.C. §§ 2702(a) for Facebook's unlawful disclosure/divulging of the content of Plaintiff's and class members' communications to third parties, including but not limited to SCL, Cambridge Analytica, Aleksandr Kogan, and GSR.

79. The Stored Communications Act ("SCA") prohibits a person from intentionally accessing without (or in excess of) authorization a facility through which an electronic

communications service is provided and thereby obtaining an electronic communication while it is in “electronic storage.” 18 U.S.C. § 2701(a).

80. The SCA defines “electronic storage” as “any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and any storage of such communication by an electronic communication service for purposes of backup protection of such communication.”

81. The servers Facebook uses to provide its electronic communications service to Facebook users are a “facility” within the meaning of the SCA.

82. Defendants are “person[s]” within the meaning of the SCA.

83. Facebook’s provision of ‘users’ personal data with third parties as alleged herein exceeded any authorization from any party to the personal data at issue.

84. Because of the architecture of Facebook’s servers, the sharing of personal data among Facebook users results in and constitutes interstate data transmissions.

85. The acquisition of Class Members’ personal Facebook data—which constitute “communications” pursuant to the SCA—by Cambridge Analytica exceeded authorization to the personal data at issue.

86. Because of the architecture of Facebook’s servers, the sharing of personal data among Facebook users results in and constitutes interstate data transmissions.

87. Pursuant to 18 U.S.C. § 2707(c), Plaintiff and class members are entitled to minimum statutory damages of \$1,000 per person, punitive damages, costs, and reasonable attorneys’ fees.

COUNT TWO

Unjust Enrichment

116. Plaintiff incorporates by reference all allegations of the preceding paragraphs as though fully set forth herein.

117. As a result of Defendant Facebook allowing third parties to access the Personal Information of Plaintiff and class members, Defendants improperly obtained and misused the Personal Information of Plaintiff and Class Members for their own benefit.

118. Defendants received millions of dollars in revenue from the sale and misuse of Plaintiff's and class members' Personal Information.

119. This revenue was a benefit conferred upon Defendants by Plaintiff and the Classes.

120. Defendants had knowledge of the monetary benefits conferred by Plaintiff and class members.

121. Defendants were unjustly enriched by retaining the revenues obtained through falsehoods, deception, and breach of trust; Plaintiff and each Class member are entitled to recover the amount by which Defendants were unjustly enriched at their expense.

122. Accordingly, Plaintiff, on behalf of class members, seek damages against Defendants in the amounts by which Defendants have been unjustly enriched at Plaintiff's and class members' expense, and such other relief as this Court deems just and proper.

COUNT THREE

Declaratory Relief 28 U.S.C. § 2201

123. Plaintiff incorporates by reference all allegations of the preceding paragraphs as though fully set forth herein.

124. An actual controversy, over which this Court has jurisdiction, has arisen and now exists between the parties relating to the legal rights and duties of Plaintiff and Defendants for which Plaintiff desires a declaration of rights.

125. Plaintiff contends and Defendants dispute that Defendants, in whole or in part, were authorized by Plaintiff and class members to acquire user data via the "friends permissions" functionality without the express consent, from each developer, of all users whose personal data was thereby acquired.

126. Plaintiff, on behalf of herself and the Class are entitled to a declaration that Defendants were *not* so authorized through their contracts with Facebook, and accordingly that Defendants' behavior violated the Stored Communications Act.

RELIEF REQUESTED

127. Plaintiff, individually and on behalf of class members, requests that the Court enter judgment in their favor and against Defendants, as follows:

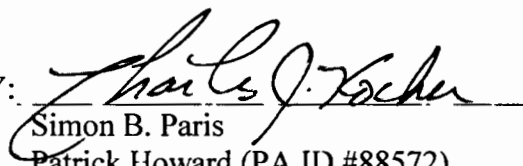
- a. Certification of the proposed classes, including designation of Plaintiff as the class representatives and appointment of Plaintiff's counsel as Class Counsel;
- b. Judgment against Defendants for Plaintiff's and class members' asserted causes of action;
- c. Appropriate declaratory relief against Defendants;
- d. Preliminary and permanent injunctive relief against Defendants;
- e. An Order of disgorgement wrongfully obtained profits;
- f. An award to Plaintiff and class members actual, statutory, and punitive damages as permitted by applicable laws;
- g. An award of attorneys' fees and other litigation costs reasonably incurred; and
- h. Any and all relief to which Plaintiff and the Class may be entitled or such other relief that the Court deems appropriate.

DEMAND FOR JURY TRIAL

Plaintiff, on behalf of herself and all others similarly situated, hereby demands a trial by jury on all the issues so triable.

DATE: June 18, 2018

BY:



Simon B. Paris

Patrick Howard (PA ID #88572)

Charles J. Kocher (PA ID #93141)

**SALTZ, MONGELUZZI, BARRETT
& BENDESKY, P.C.**

1650 Market Street, 52nd Floor

Philadelphia, PA 19103

Telephone: (215) 496-8282

Fax: (215) 496-0999

E-mail: sparis@smbb.com

E-mail: phoward@smbb.com

E-mail: ckocher@smbb.com

Attorneys for Plaintiff and Proposed Classes